OCSC

Oceania Cyber Security Centre

Expression of Interest

Small Research Grants Program

OCSC is pleased to announce an exciting opportunity to get involved in an internationally focused research project with impact and develop your CV

Building national cybersecurity capacity and resilience is a complex and multi-dimensional problem that requires a view beyond IT. For a nation, the journey toward resilience starts with the understanding of where the country stands now to inform the next steps of national plans.

The not-for-profit Oceania Cyber Security Centre (OCSC) works in partnership with its eight Victorian member universities to advance education and the cybersecurity of Australia and other nations. The OCSC also partners with the University of Oxford, to assess national cybersecurity capacity using the Cybersecurity Capacity Maturity Model for Nations (CMM).

Due to the implementation of a new corporate plan, the OCSC is now seeking Expressions of Interest for its new Small Research Grants Program.

OCSC is allocating $150,000 in the 2022/23 Financial Year to fund up to five projects with a maximum grant of $30,000 per project. More than five projects will be funded if total project budgets do not exceed $150,000.

Successfully funded projects will focus on areas which are relevant to OCSC’s corporate mission.

Projects should have an emphasis on the cybersecurity challenges facing the Indo-Pacific region. This could include examining the uptake, compliance and activities stemming from the Boe Declaration, to building fit for purpose and effective national cybersecurity functions. Preference will be given to projects which focus on the non-technical aspects of cybersecurity and related governance, policy and regulatory issues.

Interested applicants should further familiarise themselves with OCSC’s research on the connection between the United Nations’ Sustainable Development Goals (SDGs) and cybersecurity. OCSC will welcome proposals which understands this linkage and can demonstrate how the proposed research outcomes incorporates the objectives of the SDGs.

OCSC will accept applications from both individual early to mid-stage researchers, and or consortiums from any faculties of OCSC member universities.

It is anticipated that projects will commence by end-September 2022 and be completed by January 2023. Any variance to this timing must be specified in the application however all projects must be completed by 30 June 2023.

Applications will be assessed by OCSC management and its Research Council and successful applicants will be invited to present their projects to a joint meeting of the OCSC Board, Advisory Board and Research Council. Depending on the applicability of any of projects to OCSC's future activities, opportunities may present for the project to be exposed on a wider, international basis.

Selection Criteria and How to Apply

The selection criteria for these projects involve a mix of general research experience, preferable in a multi-disciplinary environment. International experience is preferred or demonstrated interest and awareness in global cyber challenges.

Each applicant should provide a one-page project outline specifying what their project is, how it aligns to OCSC's mission, what are the key cybersecurity challenges that are being addressed, and how the project may result in greater impact to improve cyber maturity and/or resilience, preferably at a country or regional-level. A separate table stating the project team and expected project costs on a time, labour and materials basis must be included.

General Selection Criteria for Research Analysis and Writing

Essential

- Demonstrated analytical skills;
- Demonstrated writing skills for non-technical audiences;
- Demonstrated ability to handle and protect confidential information;
- Demonstrated ability to meet timelines.

Highly Desirable

- Demonstrated expertise or knowledge in any of the following areas:
  - analysis or knowledge of cyber legislation and regulation; or
  - analysis of national policy; or
  - familiarity in international affairs or policy.

Additional Preferable Selection Criteria

- Demonstrated verbal communication skills;
- Demonstrated listening skills;
- Ability to act and communicate with tact and diplomacy;
- Demonstrated ability to handle and protect confidential information;
- Analysis or knowledge of cyber legislation and/or other policy and regulation.

Application process

- All OCSC member universities are encouraged to identify suitably qualified individuals from **any** faculty and submit relevant CVs and project applications.
- Each interested applicant should submit a single application including a CV and a project statement (around 1 page) outlining their project against the criteria in this EOI. Potential candidates will be shortlisted by OCSC management and may be called for interview. OCSC's Research Council will provide input into the application process.
- OCSC reserves the right to seek further information, clarification or supporting information from any applicant to verify their claims or to further assess their project proposal.
- Applications (EOIs) are to be forwarded to info@ocsc.com.au.

Project Engagement

- Successful individuals will be engaged either as project employees by OCSC for an agreed fixed fee for the duration of the project or will be engaged through funding provided directly to the applicable OCSC member university(s) via a standard project agreement including milestones and key deliverables.

Further Information

- Potential applicants should review OCSC's website (ocsc.com.au) to learn more about the Centre's mission and activities. If following review of OCSC's website, further information is required, please contact info@ocsc.com.au stating your query and we will respond either in writing or personally.

Closing date for applications: COB Monday 19 September 2022.